



## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2001147976 A**

(43) Date of publication of application: **29.05.01**

(51) Int. Cl.

**G06F 17/60**

**G06K 17/00**

**G07F 17/00**

(21) Application number: **2000257086**

(71) Applicant: **CANON INC**

(22) Date of filing: 05.09.95

(72) Inventor: **IWAMURA KEIICHI**

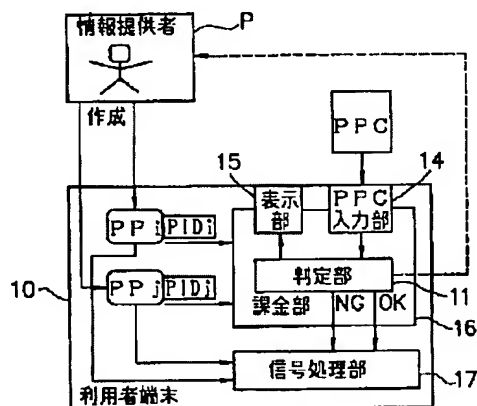
(62) Division of application: **07227843**

**(54) CHARGING DEVICE, INFORMATION RECEIVER  
AND COMMUNICATION SYSTEM**

**(57) Abstract:**

**PROBLEM TO BE SOLVED:** To easily and suitably manage charging to the information utilization of a user on a multimedia network or the like while protecting the privacy of the user.

**SOLUTION:** The user inputs the monetary information of cash, prepaid card or IC card to a PPC input part 14 provided on a user terminal 10. Then, on the basis of an amount shown by that monetary information and/or charge information PID added to provided information PP from an information provider P, a discriminating part 11 discriminates whether the provided information PP may be utilized and, corresponding to a signal permitting the utilization, the provided information PP is processed and outputted to the user by a signal processing part 17. The information and the discrimination result on the monetary information are displayed.



COPYRIGHT: (C)2001,JPO

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-147976

(P2001-147976A)

(43) 公開日 平成13年5月29日 (2001.5.29)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード*(参考)
G 0 6 F 17/60	3 0 2	G 0 6 F 17/60	3 0 2 E
	Z E C		Z E C
	3 3 2		3 3 2
	4 0 8		4 0 8
	4 1 0		4 1 0 E

審査請求 未請求 請求項の数17 O L (全 13 頁) 最終頁に続く

(21) 出願番号 特願2000-257086(P2000-257086)  
 (62) 分割の表示 特願平7-227843の分割  
 (22) 出願日 平成7年9月5日(1995.9.5)

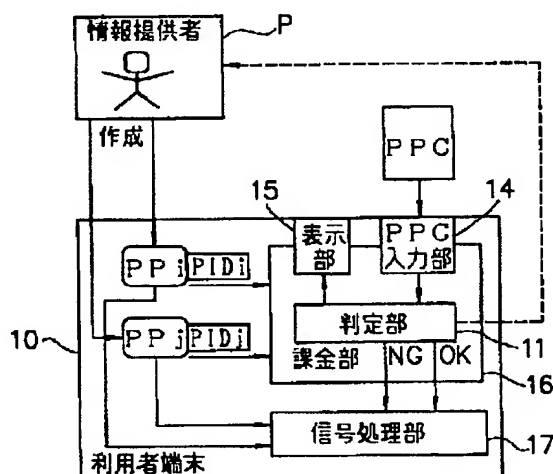
(71) 出願人 000001007  
 キヤノン株式会社  
 東京都大田区下丸子3丁目30番2号  
 (72) 発明者 岩村 恵市  
 東京都大田区下丸子3丁目30番2号 キヤ  
 ノン株式会社内  
 (74) 代理人 100090273  
 弁理士 國分 孝悦

(54) 【発明の名称】 課金装置、情報受信装置及び通信システム

## (57) 【要約】

【課題】 マルチメディアネットワーク等において利用者の情報利用に対する課金を、管理を容易に行い、かつ利用者のプライバシーを保護しながら適切に行う。

【解決手段】 利用者が利用者端末10に設けられたPPC入力部14に現金、プリペイドカード、ICカード等による金銭情報を入力すると、判定部11がその金銭情報が示す金額及び／または情報提供者Pからの提供情報PPに付加された料金情報PIDに基づいて提供情報PPの利用可否を判定し、利用を許可する信号に応じて信号処理部17が提供情報PPを処理して利用者に対して出力する。金銭情報に関する情報及び判定結果は、表示される。



## 【特許請求の範囲】

【請求項1】 記録媒体に記録され、所定の金融機関等にて保証された金額を示す金銭情報が入力される入力手段と、

上記入力手段から入力された金銭情報を判定し、情報提供者から提供される画像データ、音声データ、コンピュータデータ、コンピュータプログラム等の提供情報の利用を許可する許可信号を出力する判定手段と、

上記許可信号に応じて上記提供情報の利用が可能となるように処理する処理手段と、

上記金銭情報に関する情報及び上記判定手段による判定の結果を表示する表示手段とを備えた課金装置。

【請求項2】 上記判定手段は、上記金銭情報と上記提供情報に付加された利用料金情報とに基づいて判定を行うようにした請求項1記載の課金装置。

【請求項3】 上記金銭情報が現金である請求項1記載の課金装置。

【請求項4】 上記記録媒体はICカードである請求項1記載の課金装置。

【請求項5】 情報提供者から提供される画像データ、音声データ、コンピュータデータ、コンピュータプログラム等の提供情報を受信するように成された情報受信装置であって、

所定の金融機関等にて保証された金額を示す金銭情報が入力される入力手段と、

上記入力手段から入力された金銭情報を判定して上記提供情報の利用を許可する許可信号を出力する判定手段と、

上記許可信号に応じて上記提供情報の利用が可能となるように処理する処理手段と、

上記金銭情報に関する情報及び上記判定手段による判定の結果を表示する表示手段とを備えた情報受信装置。

【請求項6】 上記判定手段は、上記金銭情報と上記提供情報に付加された利用料金情報とに基づいて判定を行うようにした請求項5記載の情報受信装置。

【請求項7】 上記金銭情報が現金である請求項5記載の情報受信装置。

【請求項8】 上記金銭情報は記録媒体に記録された情報である請求項5記載の情報受信装置。

【請求項9】 上記提供情報の利用情報を外部に送信する通信手段を備えた請求項5記載の情報受信装置。

【請求項10】 情報を提供する情報提供者端末装置と、

上記情報提供者端末装置からの画像データ、音声データ、コンピュータデータ、コンピュータプログラム等の提供情報を受信して利用する利用者端末装置と、

所定の金融機関等にて保証された金銭情報を入力するように成され、入力された金銭情報を判定して上記提供情報の利用を許可する許可信号を出力する判定手段と上記許可信号に応じて上記提供情報の利用が可能となるよう

に処理する処理手段と上記金銭情報に関する情報及び上記判定手段による判定の結果を表示する表示手段とを有する課金装置とを備えた通信システム。

【請求項11】 上記判定手段は、上記金銭情報と上記提供情報に付加された利用料金情報とに基づいて判定を行うようにした請求項10記載の通信システム。

【請求項12】 上記金銭情報が現金である請求項10記載の通信システム。

【請求項13】 上記金銭情報は記録媒体に記録された情報である請求項10記載の通信システム。

【請求項14】 上記利用者端末装置に提供情報の利用情報を送信する通信手段を設けた請求項10記載の通信システム。

【請求項15】 上記利用情報に応じて上記情報提供者端末装置に料金分配情報を送信する料金分配者端末装置を設けた請求項14記載の通信システム。

【請求項16】 上記利用情報に応じて提供情報の利用料金の立替え処理を行う料金立替端末装置を設けた請求項14記載の通信システム。

【請求項17】 上記各装置間の通信を暗号通信により行うようにした請求項10、14～16の何れか1項記載の通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、動画像データ、静止画像データ、音声データ、コンピュータデータ、コンピュータプログラム等の情報を伝送するマルチメディアネットワーク等で用いられる課金装置、情報受信装置及び通信システムに関し、特に情報の提供とそれに対する課金方式に関するものである。

【0002】

【従来の技術】近年、幹線通信網における光ファイバネットワークの整備、ケーブルテレビシステムの普及、衛星通信の実用化、ローカルエリアネットワークの普及等に伴い、かかる通信網を利用して様々な情報を提供し、その情報の内容及び量に応じて料金を徴収する、いわゆる情報サービス産業が増大している。このようなサービスにおいては、提供した情報に対する課金を適切に行うことが重要となる。

【0003】しかしながら、現実では情報の保護は不完全であり、プログラムや映像（音声を含む）情報の不正利用が問題になっている。この不正利用を防ぐために、コピー防止機能を付けたり、コンピュータ等に付与されているハードウェア機番を用い、ソフトウェア自体に上記機番に相当するソフトウェア機番を付与し、プログラム実行時に、2つの機番を照合する等の手法がある。しかし、コピー防止機能はバックアップ等の際不便であり、機番照合は機番管理や販売に関して不便であり、あまり実用的ではなかった。

【0004】これに対して、「超流通」というソフトウ

ウェア権利者（以後、情報提供者）の権利の保護をめざした概念が森亮一氏によって提案され、特開昭60-77218号、特開昭60-191322号、特開昭64-68835号、特開平02-44447号、特開平04-64129号等の各公報に示された。図10は特開平04-64129号公報に示された「超流通」の概念図である。情報提供者Pは自分が作成したソフトウェアP P i（またはP P j）を利用者端末10に送る。利用者端末10はソフトウェアP Pの利用可否を、ソフトウェアP Pに付加された固有データP I D i（またはP I D j）と利用者のユーザI D毎の条件によって判定部11で判定し、利用可ならば提供情報の利用履歴を記憶部12に記録し、その履歴に基づいて情報提供者Pはその提供情報（ソフトウェアP P）の利用料金等を請求する。13は以上の各部を含むS S U（ソフトウェアサービスユニット）である。

【0005】

【発明が解決しようとする課題】しかしながら上述した「超流通」方式は次のような問題点があった。

（1）「超流通」は情報提供者に許可された利用者であるかどうかをユーザI D等の利用者固有データによって判定し、そのために「超流通」を実現するには、少なくとも利用者固有データの格納手段を設ける必要がある。このような方式では、利用者は予め情報提供者に情報の利用を申し込み、自分のユーザI D等をもらい、一利用者固有データとして登録する必要がある。このような利用申し込みの手続きや、ユーザI Dのような多くの異なる利用者固有データを管理することは煩雑である。

【0006】（2）「超流通」は情報の不正利用を防止するため、または情報提供者が自分の提供情報の利用状況を把握するために、記憶部12のような利用ソフトウェア履歴格納手段を備え、その履歴に基づいて情報提供者が利用者に料金の請求等を行う。「超流通」において情報は買い取りではなくレンタル的な扱いをするために、この利用履歴は必要になるが、このような方式では、利用者がどのような情報を利用したかということが情報提供者に知られてしまい、利用者のプライバシーを保護することができない。

【0007】（3）「超流通」は提供情報の利用状態を正しく把握する、すなわち、利用料金を正しく把握するための方式ではあるが、料金の支払いに関する手段や方式は含まれていない。このため情報提供者が提供情報の利用状態を知った後は、他の手段によって料金の請求及び徴収を行う必要がある。

【0008】本発明は上述のような実情に鑑みてなされたものであり、前述の（1）～（3）の問題を解決することのできる課金方式を提供することを目的とする。

【0009】

【課題を解決するための手段】請求項1の発明による課金装置においては、記録媒体に記録され、所定の金融機

関等にて保証された金額を示す金銭情報が入力される入力手段と、上記入力手段から入力された金銭情報を判定し、情報提供者から提供される画像データ、音声データ、コンピュータデータ、コンピュータプログラム等の提供情報の利用を許可する許可信号を出力する判定手段と、上記許可信号に応じて上記提供情報の利用が可能となるように処理する処理手段と、上記金銭情報に関する情報及び上記判定手段による判定の結果を表示する表示手段とを設けている。

10 【0010】請求項5の発明による情報受信装置においては、情報提供者から提供される画像データ、音声データ、コンピュータデータ、コンピュータプログラム等の提供情報を受信するように成された情報受信装置であって、所定の金融機関等にて保証された金額を示す金銭情報が入力される入力手段と、上記入力手段から入力された金銭情報を判定して上記提供情報の利用を許可する許可信号を出力する判定手段と、上記許可信号に応じて上記提供情報の利用が可能となるように処理する処理手段と、上記金銭情報に関する情報及び上記判定手段による判定の結果を表示する表示手段とを設けている。

20 【0011】請求項10の発明による通信システムにおいては、情報を提供する情報提供者端末装置と、上記情報提供者端末装置からの画像データ、音声データ、コンピュータデータ、コンピュータプログラム等の提供情報を受信して利用する利用者端末装置と、所定の金融機関等にて保証された金銭情報を入力するように成され、入力された金銭情報を判定して上記提供情報の利用を許可する許可信号を出力する判定手段と上記許可信号に応じて上記提供情報の利用が可能となるように処理する処理手段と上記金銭情報に関する情報及び上記判定手段による判定の結果を表示する表示手段とを有する課金装置とを設けている。

【0012】

【作用】本発明によれば、現金あるいはプリペイドカード等の記録媒体に記録され、所定の金融機関等にて保証された金銭情報に基づいて判定手段は利用者の画像データ、音声データ、コンピュータデータ、コンピュータプログラム等の提供情報の利用可否を判定し、利用可のとき許可信号を出力し、この許可信号に応じて提供情報の利用が可能となるように処理することにより、利用者は利用者端末等を動作させることで提供情報を得ることができる。また、利用可能な残高等の金銭情報に関する情報を表示するので、利用者はあとどれくらい使用できるのか予め知ることができる。更に、判定の結果を表示することで利用者は自分が欲した情報を利用できるのか否かを直ちに知ることができる。

【0013】

【発明の実施の形態】以下、本発明に係る第1の実施の形態を図1を参照して説明する。図1において、10は情報受信装置としての利用者端末、Pは情報提供者、P

Pi (またはPPj) は情報提供者Pによって有償で提供される提供情報、PIDi (またはPIDj) はPPiに付加された固有の情報固有データ、PPCは後述するように現金やカード等に記録された金銭情報、14はPPCの入力部、15は表示部、16は上記各部14、15及び判定部11を含む課金部、11は提供情報PPの利用可否を判定する判定部、17は信号処理部である。

【0014】次に動作について説明する。情報提供者PはPIDを含めた提供情報PPを提供する。利用者端末10は、その提供情報PPを利用する際には、必ず課金部16を経由するように構成してある。この課金部16は金銭情報であるPPCの受け口としての入力部14がある。提供情報PPの利用要求が生じると、判定部11はPID及び／またはPPCに基づいて、提供情報PPの利用可能性をチェックする。例えば、PIDに示された利用料金がPPCの金銭情報が示す残高以内か否かなどのチェックである。利用がOK (許可) か否 (NG) かは信号処理部17に通知され、もしOKであれば、信号処理部17は利用者が提供情報PPの利用が可能となるように処理して出力する。このときのPIDやPPCに関する情報 (提供情報の利用料金やPPCの残高など) は表示部15で表示される。また、判定部11の利用可否の判定結果も表示部15で表示することができる。

【0015】本発明における金銭情報PPCは実際の金銭 (現金) であってもよいし、テレホンカードのようなプリペイドカードであってもよいし、フロッピー (登録商標) ディスク及びICカードやPCMCIAなどに格納された金銭と等価な電子的な情報であっても良い。本発明では、利用者毎の利用者固有データとしてのユーザIDを用いず、その代わりに利用者に依存しない金銭情報PPCによって提供情報PPの利用可否を判定する。従って、利用者はユーザIDをもらうための申し込み手続きをする必要が無く、実際の金銭と等価な金銭情報PPCをもつだけ、即ち利用する情報に対する料金を支払うだけであるので、自然であり容易である。これによって、多くの利用者固有情報を管理する必要もなくなり前記(1)の問題が解決される。

【0016】また、本発明では利用者固有データを持たないため、利用者は自分がどの情報を利用したかというプライバシーを情報提供者に知られることはない。これは情報提供者Pの権利が守られていないように見えるが、自分の提供情報の利用頻度に応じた料金が支払われさえすれば情報提供者Pには十分であって、どの利用者かどの情報を利用したかという利用者のプライバシーまで知る必要はない。本発明では、どのユーザIDをもつ利用者がどの情報PIDを利用したかという利用履歴格納手段はもたないが、どの情報が何度利用されたかという利用頻度格納手段または現在提供情報を利用している

10

20

30

40

50

ことを知らせる利用通知手段を有することはできる。図1においては、点線で示す経路によって情報提供者Pに利用頻度情報が知らされる。なお、具体的な利用頻度格納手段または利用通知手段については後述する第2～6の実施の形態で詳述する。以上により、前記(2)の利用者のプライバシーの問題も解決される。

【0017】本発明では、PPCは金銭と等価な情報であるので、PPCを用いること自体が料金の支払いに相当する。これによって前記(3)の問題も解決される。なお、具体的なPPCの入手法と回収法、及び料金の分配法は前記(2)の問題と絡めて第2～6の実施の形態に示される。

【0018】尚、課金部16は本発明の課金装置であり、これを図1では利用者端末10の内部に一体的に設けているが、課金部16を利用者端末10とは別体に設けてもよい。その場合、情報提供者Pから提供情報PPに付加された情報PIDを課金部16が先ず受信し、PID、PPCに基づく判定部11の判定結果がOKであることを示す信号に基づいて利用端末装置10に対して提供情報PPの受信や信号処理を許可するような構成としてよい。また、このような構成は、後述する第2～第8の実施の形態に適用してよい。

【0019】次に第2の実施の形態を図2について説明する。図2はPPCが実際の金銭 (現金) である場合を示す。この場合のPPCの入力部14はコインや紙幣の入口であり、利用者はまずこの入力部14に一定の金銭を入れる。その金銭がPIDに示された料金を超えたときに判定部11は提供情報PPの利用を許可する。または、課金部16は表示部15により利用者に提供情報の利用料金を表示し、利用者はそれに相当する金銭をPPCの入力部14に入力する。判定部11はそれをもとに提供情報PPの利用可否を判定する。また、時間に応じて料金が更新される場合には、その旨を表示し、それに応じた追加料金を入力するようにしてもよい。また、入力された金額はコインボックス18に格納され、情報提供者Pまたは料金の回収を行う何らかの機関が回収する。このとき、各提供情報PP毎の利用頻度はカウンタ19に記録・回収され、その利用頻度に応じてコインボックス18の料金が各情報提供者Pに分配される。提供情報PPが一つである場合等、利用頻度が不要ない場合にはカウンタ19は省略できる。

【0020】次に第3の実施の形態を図3について説明する。図3はPPCがテレホンカードのようなプリペイドカードである場合を示している。利用者はPPCの入力部14にプリペイドカードをさし込み、それに記載された金額がPIDに示された利用料金 (この金額は表示されてもよい) より多いか否かを判定部11が判定し、多い場合にはPPの利用を許可する。この場合、PPの利用料金が時間によって更新されていっても、プリペイドカードの料金内であれば継続して利用可能となるよう

に、判定部11とPPCの入力14は構成される。入力部14がプリペイドカードを追加して挿入できる構成とした場合はさらなる長時間の利用も可能となる。

【0021】このようなプリペイドカードの入手は現在のテレホンカードと同様に多くの販売店によって市販される販売形態になっていればどこでも容易に入手可能である。この場合、プリペイドカードの製造会社は料金分配者20となり、情報提供者Pはその料金分配者20に登録することによって提供情報PPの利用頻度に応じた料金の分配を受ける。前述の販売店は料分配者に含まれる。

【0022】この利用頻度に応じた料金の分配は、課金部16が通信I/F21を用いて現在の利用情報を料金分配者20に知らせることによって実現される。この利用通知は課金部16がプリペイドカードの金額を更新するときに限り出力されるように構成される。提供情報PPを通信によって入力する場合は、この通信I/F21を共有することができる。この場合、図4に示されるように料金分配者20の端末、情報提供者Pの端末及び利用者端末10はネットワーク22に接続されており、料金分配者20は上記通知に応じて料金を情報提供者Pに分配する。

【0023】また、通信I/F21を持たない場合は、利用する情報に応じてプリペイドカードの種類を変えるという方法もある。このとき、判定部11は情報に応じてプリペイドカードの種類を調べるという処理を行い、それに対する利用可否も判定する。また、課金部16に提供情報PPの利用記録をプリペイドカードに記録する手段を設け、このプリペイドカードを料金分配者20が回収することによって、利用頻度に応じた料金の分配を行うこともできる。その場合、プリペイドカードの回収を促進するために、プリペイドカードの交換の場合は、金銭情報のみの料金で済み、プリペイドカードの交換でない場合は、金銭情報の料金の他にプリペイドカード自体の料金も加算されるなどの販売形態にすればよい。ただし、回収できない利用記録に対応する料金は回収できない利用記録に応じた比率で分配しても良い。

【0024】図5は第4の実施の形態を示すもので、PPCがフロッピーディスクまたは書き換えが容易な電氣的及び／または磁氣的なデバイスである場合を示す。また、ネットワークシステムを図6に示す。この場合、PPC内に格納される金銭情報は銀行やその他の金融機関等によって保証されたデータであったり、販売店を含む料金分配者20によってのみ加算処理できる特殊なデータである。利用者は入力部14にPPCをさし込む。課金部16はPPCから情報を読み出し、その金額がPIDに示された料金より多く（この金額は表示されてもよい）、課金部16がPPCに利用料金を請求可能である場合に判定部11はPPの利用を許可（OK）する。この場合、PPの利用料金が時間によって更新されてい

ても、PPCの記載料金以内は継続して利用可能であるように構成される。

【0025】この場合の金銭情報は電子的な情報であるので、金銭情報の入出力も通信I/F21を介して料金分配者20との所定の手続きによる通信によって行うことができる。このとき、第1、第2の実施の形態と異なり、実際の金銭を利用者は料金分配者20に直接支払うわけではないので、利用者の金銭支払いを保証するのは利用者と契約を結んだ銀行やその他の金融機関（以後、料金立替者23）である。さらに、利用情報の通知に関しても、第3の実施の形態と同様に通信I/F21を用いて現在の利用情報を料金分配者20に知らせることによって、利用頻度に応じた料金の分配が可能になる。この場合、利用料金を電子的な金銭情報PPCによって直接料金分配者20や情報提供者Pに送ることも可能である。

【0026】具体的には、次のような通信処理によって電子的な金銭情報の入出力が実現できる。また、課金部16は後述のような暗号・認証処理手段を有しており、後述するTA等で示されるタイムスタンプを安全に管理する手段を有するものとする。これは、PPCがフロッピーディスク等の書き換えが容易な媒体であるために、PPCのコピー等によって不正が行われる可能性があるため、それを防止するためにPPCを認証可能にし、タイムスタンプの管理によってPPCのコピー等の不正に対抗するものである。

【0027】次に、利用者をA、情報提供者をB、料金分配者をC、料金立替者をDとし、各々は署名可能な秘密鍵を秘密に保持し、通信相手はその署名を検査できる公開鍵を知っているもの（例えば、Aの秘密鍵をsA、公開鍵をpAとする）として課金処理を説明する。ここで、AがBの提供情報Piを利用する場合を考える。ただし、Xの鍵Yによる処理結果を{X}^Yで表し、利用者の各処理及び鍵やタイプスタンプの管理は課金部16内の安全性が保証された手段または各人の記憶や記録によるものとする。

【0028】[金銭情報入手処理]

(1) Aはa円（通貨の単位は円に限らない）分の金銭情報の入力要求を自分の登録情報iA（口座番号やクレジット番号など）をつけて秘密鍵sAで署名しCに送る。

$MA = \{A, \{A, iA, a, TA\}^{sA}\}$

【0029】(2) CはMAの署名をAの公開鍵pAで検査し、iAを用いてDにa円分の請求を行い、それが受け入れられれば金銭情報aを1円毎または基本単位c毎（情報が100円単位の価格であれば100円毎）にCの署名鍵であるsCで署名して次のメッセージをAに送る。ただし、それらには異なるタイムスタンプTCiがつけられる。

$MC = \Sigma \{TA, \{C, e, TCi\}^{sC}\}^{pA}$

【0030】(3) AはMCの各々を $pA$ で復号し、さらに $sC$ に対応するCの公開鍵 $pC$ で署名を検査し、検査結果が正しければ $\{C, a, TCi\} \wedge sC$ をPPCに記録する。なお、 $TA, TCi$ はタイムスタンプを示すものであり、同じ送信者からの同じタイムスタンプをもつメッセージは不正要求とする。また、 $TA, TCi$ はシリアル番号や偶然一致することがないまたは少ない乱数のようなものであればタイムスタンプでなくてもよい。

#### 【0031】[利用情報通知処理]

(1) Aが情報 $Pi$ を利用したいとき、AのPPC内の金銭情報が $PIDi$ に示された利用料金より大きければ課金部16は $Pi$ の利用を許可する。

(2) Aが $Pi$ の利用を終了したとき、または利用中に課金部16はPPCの金銭情報から要した利用料金を消去する。

【0032】(3) このとき、Aは次の利用通知MBをCに送る。ただし、消去された利用料金を $b$ とする。

$MB = \{A, B, \{B, b, TB\} \wedge sA\}$

(4) Cはこのメッセージを検査し正しいときに、 $b$ 円をBへの分配金として支払う。

【0033】上記の説明では、処理を簡単にするためにCと各利用者間の暗号方式は公開鍵暗号としたが、予め鍵が共有されていれば共通鍵暗号を用いてもよいことは明らかである。また、タイムスタンプからの時間によって各メッセージの有効期間を定めることもできる。以上において、メッセージ内の並び順は順不同であり、A、B等で示す利用者の識別子やタイムスタンプは必ずしも必要でない場合もある。さらに、上記の金銭情報入手処理、利用情報通知処理の手順は1つの例であり、電子的な情報を金銭情報として利用者固有データを用いずに課金処理を行うものは全て本発明に含まれる。

【0034】また、通信 $I/F21$ を持たない場合、利用者は販売店などの料金分配者20のところでPPCに格納する金銭情報を料金と引き替えに入力してもらう。また、課金部16が前記MBのような提供情報PPの利用記録をPPCに記録し、PPCを販売店等の料金分配者20のところで金銭情報を補充・入力する際に利用記録を補充器が回収することによって、利用頻度に応じた料金の分配を行うようにすることができる。このような電子的な金銭情報は前述したように料金分配者20だけが処理できる特殊なデータであるので、通信 $I/F21$ を持たない利用者はPPCを用いるためには必ず販売店等の料金分配者20を介する必要があるので、利用記録は必ず回収でき利用頻度に応じた料金の分配が可能である。

【0035】図7は第5の実施の形態を示すもので、PPCがICカードやPCMCIAのような電子的なカードである場合を示す。ネットワークシステムの構成は図6と同一である。この場合は、PPC内に格納される金

銭情報は銀行やその他の金融機関等によって保証されたデータであったり、販売店を含む料金分配者20によってのみ加算処理できる特殊なデータである。利用者はPPCの入力部14にPPCをさし込み、所定の手続き（暗証番号の検査など）によってPPCを動作可能にする。課金部16はPPCから金銭情報を読み出し、その額が $PID$ に示された料金より多く（金額は表示されてもよい）、課金部16がPPCに利用料金を請求可能である場合に判定部11はPPの利用を許可する。この場合、PPの利用料金が時間によって更新されていても、PPCの記載料金以内は継続して利用可能であるように構成される。

【0036】この場合の金銭情報は電子的な情報であるので、金銭情報の入出力も通信 $I/F21$ を介して料金分配者20との所定の手続きによる通信により行うことができる。このとき、第1、第2の実施の形態と異なり実際の金銭を利用者は料金分配者20に直接支払うわけではないので、利用者の金銭支払いを保証するのは利用者と契約を結んだ銀行やその他の金融機関、即ち、料金立替者23である。さらに、利用情報の通知に関しても、第3の実施の形態と同様に通信 $I/F21$ を用いて現在の利用情報を料金分配者20に知らせることによって、利用頻度に応じた料金の分配が可能になる。この場合、利用料金を電子的な金銭情報によって直接料金分配者20や情報提供者Pに送ることも可能である。

【0037】具体的には、次のような通信処理によって電子的な金銭情報の入出力が実現できる。ただし、通信や処理に関する安全性を考慮してPPCとして用いる電子的なカードはセキュリティ機能として暗証番号による所有者確認や、アクセス条件によるデータメモリへのアクセス制御や、後述のような暗号方式による暗号・認証を行うことができるものとする。このとき、暗号処理や認証処理に用いる秘密鍵は前述のようにアクセス制御されたメモリ領域に書き込まれ、そのアクセス条件を満たす者（カード発行者や料金分配者等）しかアクセスできないものとする。また、以下の課金動作もカードの発行者または料金分配者20以外変更できない仕様になっているものとする。

【0038】利用者端末10、情報提供者Pの端末、料金分配者20の端末、料金立替者23の端末は図6のようにネットワーク22で接続されている。ここで、利用者をA、情報提供者をB、料金分配者をC、料金立替者をDとし、Cは各利用者に対して暗号通信のための秘密鍵を共有し（例えば、AとCの間の秘密鍵を $sA$ 、BとCの間の秘密鍵を $sB$ とする）、Cは自分しか知らない署名のための秘密鍵 $sC$ を秘密に保持し、それに対応する署名の検査鍵 $pC$ を公開しているものとする。以下に、AがBの提供情報 $Pi$ を利用する場合を考える。ただし、平文Xの鍵Yによる暗号文を $\{X\} \wedge Y$ で表し、利用者の各処理は全て上述のようなセキュリティ機能を

10

20

30

40

50



もつPPC内で行われるものとする。

【0039】[金銭情報入手処理]

(1) AはCにa円(通貨の単位は円に限らない)分の金銭情報の入力要求をDへの自分の登録情報iA(口座番号やクレジット番号など)をつけてCに送る。

$MA = \{A, \{A, iA, a, TA\} \wedge sA\}$

【0040】(2) CはMAの暗号部分をAと共有しているsAで復号し、iAを用いてDにa円分の請求を行い、それが受け入れられれば金銭情報aにCの署名鍵であるsCで署名して次のメッセージをAに送る。

$MC = \{TA, \{C, a, TC\} \wedge sC\} \wedge sA$

【0041】(3) AはMCをsAで復号し、さらにsCに対応するCの公開鍵pCで署名を検査し、検査結果が正しい場合のみAのPPCはa円分の金銭情報を加算する。上記TAやTCはタイムスタンプであり、同じ送信者からの同じタイムスタンプをもつメッセージは不正要求とする。また、TA、TCはシリアル番号や偶然一致することがないまたは少ない乱数のようなものであればタイムスタンプでなくてもよい。

【0042】[利用情報通知処理]

(1) Aが情報Piを利用したいとき、AのPPC内の金銭情報がPIDiに示された利用料金より大きければ課金部16はPiの利用を許可する。

(2) AがPiの利用を終了したとき、または利用中に課金部16はPPCの金銭情報から要した利用料金を差し引き、その結果をPPCに書き込む。

【0043】(3) このとき、Aは次の利用通知をCに送る。ただし、差し引いた利用料金をbとする。

$MB = \{A, \{B, b, TB\} \wedge sA\}$

(4) Cはこのメッセージを復号し正しいときに、b円をBへの分配金として支払う。

【0044】次に、AとBの間の情報も暗号通信によってやりとりする場合、次の処理を前述の金銭情報入手処理と利用情報通知処理の間で行えばよい。ただし、Cは情報提供者とも秘密鍵を共有しているとする。

【0045】[情報利用処理](1) AはCにBとの会話鍵の生成を依頼するために次のメッセージをCに送る。

$MA' = \{A, B, TA'\}$

(2) Cは会話鍵CKを生成し、次のメッセージをAに送る。

$MC' = \{\{TC', A, CK\} \wedge sB, TA', B, CK\} \wedge sA$

【0046】(3) AはMC'をsAで復号し、 $\{TC', A, CK\} \wedge sB$ をBに送る。

(4) Bは受信メッセージをsBで復号し、会話鍵CKで暗号化した情報をAに送る。

(5) Aは会話鍵CKで暗号化情報を復号する。

【0047】上記の説明では、処理を簡単にするためにCと各利用者間の暗号方式は共通鍵暗号としたが、第5

の実施の形態と同様に公開鍵暗号を用いてもよいことは明らかである。また、タイムスタンプからの時間によって各メッセージの有効期間を定めることもできる。また、メッセージ内の並び順は順不同であり、A、B等で示す利用者の識別子やタイムスタンプは必ずしも必要でない場合もある。さらに、上記の金銭情報入手処理、利用情報通知処理の手順は1つの例であり、電子的な情報を金銭情報として利用者固有データを用いずに課金処理を行うものは全て本発明に含まれる。

10 【0048】また、通信I/F21を持たない場合、利用者は販売店などの料金分配者20のところでPPCに格納する金銭情報を入力してもらう。また、課金部16が提供情報PPの利用記録をPPCに記録し、このPPCを販売店等の料金分配者20のところで金銭情報を補充・入力する際に利用記録を補充器が回収することによって、利用頻度に応じた料金の分配を行うようにすることができる。このような電子的な金銭情報は前述したように料金分配者20だけが処理できる特殊なデータであるので、通信I/F21を持たない利用者はPPCを用いるためには必ず販売店等の料金分配者20を介する必要があるので、利用記録は必ず回収でき利用頻度に応じた料金の分配が可能である。

20 【0049】図8は第6の実施の形態を示すもので、第5の実施の形態と同様に電子的な情報を金銭情報として用い、料金分配者20のいろいろな課金方式を示すものである。利用者端末10、情報提供者Pの端末、料金立替者23の端末は図9のようにネットワーク22で接続されている。さらに、PPCとして用いる電子カードはセキュリティ機能として暗証番号による所有者確認や、アクセス条件によるデータメモリへのアクセス制御や、暗号方式による暗号・認証を行うことができるものとする。このとき、暗号処理や認証処理に用いる秘密の鍵は前述のようにアクセス制御されたメモリ領域に書き込まれているとする。また、以下の課金動作もカードの発行者以外変更できない仕様になっているとする。

【0050】利用者をA、情報提供者をB、料金立替者をDとし、各々は署名可能な秘密鍵を秘密に保持し、通信相手はその署名を検査できる公開鍵を知っているもの(例えば、Aの秘密鍵をsA、公開鍵をpAとする)とする。ここで、AがBの提供情報Piを利用する場合を考える。ただし、Xの鍵Yによる処理結果を $\{X\} \wedge Y$ で表し、利用者の各処理は全て上述のようなセキュリティ機能をもつPPC内で行われるものとする。

【0051】[金銭情報入手処理]

(1) Aはa円(通貨の単位は円に限らない)分の金銭情報の入力要求を自分の登録情報iA(口座番号やクレジット番号など)をつけて秘密鍵sAで署名しDに送る。

$MA = \{A, \{A, iA, a, TA\} \wedge sA\}$

【0052】(2) DはMAの署名をAと公開鍵pAで



検査し、 $iA$ が正しく $A$ が $a$ 円支払可能であれば、金銭情報 $a$ を $D$ で署名して次のメッセージを $A$ に送る。

$MD = \{TA, \{D, a, TD\}^s D\}^s A$

【0053】(3)  $A$ は $MD$ を $pA$ で検査し、さらに $sD$ に対応する $D$ の公開鍵 $pD$ で署名を検査し、検査結果が正しい場合のみ $A$ の $PPC$ は $a$ 円分の金銭情報を加算する。上記、 $TA$ や $TD$ はタイムスタンプであり、同じ送信者からの同じタイムスタンプをもつメッセージは不正要求とする。また、 $TA$ 、 $TD$ はシリアル番号や偶然一致することがない、または少ない乱数のようなものであれば、タイムスタンプでなくてもよい。

【0054】[利用情報通知処理]

(1)  $A$ が情報 $Pi$ を利用したいとき、 $A$ の $PPC$ 内の金銭情報が $PIDi$ に示された利用料金より大きければ課金手段は $Pi$ の利用を許可する。

(2)  $A$ が $Pi$ の利用を終了したとき、または利用中に課金部16は $PPC$ の金銭情報から要した利用料金を差し引き、その結果を $PPC$ に書き込む。

【0055】(3) このとき、 $A$ は次の利用通知 $MB$ を $B$ に送る。ただし、差し引いた利用料金を $b$ とする。

$MB = \{A, B, \{B, b, TB\}^s A\}$

(4)  $B$ は署名を検査し正しいときに、 $A$ の署名 $\{B, b, TB\}^s A$ を $D$ に示し、 $b$ の料金を受け取る。

【0056】次に、 $A$ と $B$ の間の情報も暗号通信によってやりとりする場合、直接相手の公開鍵で公開鍵による暗号通信を行うこともできるが、情報量が多い場合次のように共通鍵暗号による暗号通信を行うこともできる。この場合、各利用者と情報提供者の間には共通鍵暗号手段が共有されているとする。ただし、下記の(1)、

(2)において $A$ と $B$ は逆であっても良い。

【0057】[情報利用処理]

(1)  $A$ は $B$ との共通鍵 $CK$ を $B$ の公開鍵 $pB$ で暗号化して送る。

$MA' = \{A, B, CK, TA'\}^p B$

(2)  $B$ は受信メッセージを $sB$ で復号する。

(3)  $B$ は共通鍵 $CK$ で共通鍵暗号化した情報を $A$ に送る。

(4)  $A$ は共通鍵 $CK$ で共通鍵暗号化情報を復号する。

【0058】上記の説明では、説明を簡単にするために $D$ と各利用者と情報提供者 $P$ との暗号方式は公開鍵暗号としたが、前述のような共通鍵暗号を用いてもよいことは明らかである。また、タイムスタンプからの時間によって各メッセージの有効期間を定めることもできる。また、メッセージ内の並び順は順不同であり、 $A$ 、 $B$ 等で示す利用者の識別子やタイムスタンプは必ずしも必要でない場合もある。さらに、上記の金銭情報入手処理、利用情報通知処理の手順は1つの例であり、電子的な情報を金銭情報として利用者固有データを用いずに課金処理を行うものは全て本発明に含まれる。

【0059】次に、その他の実施の形態を説明する。

第7の実施の形態

第2の実施の形態に示す実際の金銭を用いた課金方式によって、1つ以上の利用者端末10を設置した施設を情報提供者 $P$ または料金分配者20が営業し、公衆電話やゲームセンター、喫茶店、図書館のように多くの人が金銭を支払うことによって自由に利用者端末10を使用するという課金システムが実現できる。

【0060】また、第3の実施の形態に示すプリペイドカードを用いた課金方式によって、情報提供者 $P$ が $CD-ROM$ やパソコン通信等によって広く提供情報 $PP$ を配布し、情報に対する著作権協会のような機関が料金分配者20となってプリペイドカードを製作・販売し、利用者は販売店などを通じてプリペイドカードを購入し、自宅やその他の端末等で提供情報 $PP$ を利用するという課金システムが実現できる。

【0061】第4の実施の形態に示すフロッピーディスクを用いた課金方式によって、第3の実施の形態における $PPC$ のための特殊な入力部14を必要とせず(利用者端末には通常フロッピーディスクの入力部14はついていないとする)、さらに金銭情報の通信によるやりとりによって販売店を省略可能とし、暗号・認証処理をソフト的に行うことによって現在のネットワークで容易に実現可能な課金システムが構成できる。

【0062】第5の実施の形態に示すICカードやPCMCIA等の電子的なカードを用いた課金方式によって、上記第4の実施の形態を用いた課金システムをより安全にした課金システムが実現できる。第6の実施の形態に示す課金方式によって、料金分配者20のいらない、即ち利用者と情報提供者 $P$ とが料金立替者23を通して直接取引をする課金システムが実現できる。また、この課金方式及び課金システムは将来実用化されると思われるある特殊なデータを金銭と同様に扱う電子現金に対しても適用可能であることは明らかである。さらに、上記の課金方式、及び課金システムを組み合わせた種々の課金システムも本発明に含まれる。

【0063】第8の実施の形態

現在、情報提供者が多くの情報を異なる鍵で暗号化して $CD-ROM$ 等に納め、媒体としての $CD-ROM$ 自体は販売店を通じて安価に販売し、利用者からの依頼に応じて情報提供者が利用者に指定情報の暗号鍵を知らせるときにその情報の利用対価を請求する課金方式が知られている。しかし、この方式では $CD-ROM$ を販売する販売店は媒体としての販売利益は得られても、提供情報を販売したことに対する利益は得られないと言う問題がある。

【0064】そこで、本発明で示した $PPC$ による課金方式をレンタル的な情報の利用ではなく、情報の買い取りに対して用いることによって上記の問題が解決できる。即ち、利用者は販売店で $CD-ROM$ 購入と同時に、プリペイドカード等の $PPC$ も購入し、情報提供者

との通信（電話など）によって暗号鍵を知るときにプリペイドカードでの支払を指定することによって、情報提供者はそのプリペイドカードを販売した販売店から利用料金を回収する。これによって、情報の利用料金の流れに対しても販売店を経由するので、販売店は情報利用に対する利益も得ることができる。その場合、課金部16はPPCの金銭情報を検査し、情報の利用が可能であれば、情報に対する暗号化を復号するときだけPPCから料金を引くように構成する。さらに、このPPCは使用しないときには換金できるとする。このとき、PPCは情報提供者毎に製作され、販売店を通じてCD-ROMと同様に販売される。従って、この実施の形態では料金分配者20は必要としない。

【0065】また、第3の実施の形態において利用情報通知処理を以下のようにすることで、プリペイドカードの利用情報通知処理も安全にすることができる。ただし、プリペイドカードにはプリペイドカード毎の識別番号*iP*とそれに対応した秘密鍵*sP*とが登録されているものとする。

【0066】[利用情報通知処理]

(1) AのPPC内の金銭情報が*PIDi*に示された利用料金より大きければCHECKは情報*Pi*の利用を許可する。

(2) Aが*Pi*の利用を終了したとき、または利用中にCHECKはPPCの金銭情報から要した利用料金を差し引き、その結果をPPCに書き込む。

【0067】(3) このとき、CHECKは次の利用通知をCに送る。ただし、Bへの利用料金を*b*とする。

$MB = \{iP, \{B, b, iP, TB\}^{sP}\}$

(4) CはMBを登録した秘密鍵*sP*で復号し、このメッセージが正しいときに*b*円をBへ分配金として支払う。これによって、*iP*と*sP*を知るもの以外、利用通知を生成することはできない。

【0068】次に、共通鍵暗号方式及び公開鍵暗号方式について説明する。

[共通鍵暗号方式] 共通鍵暗号方式は送信者と受信者で同一の暗号鍵を秘密に共有する暗号方式（秘密鍵暗号方式、対称暗号方式、慣用暗号方式とも呼ばれる）である。共通鍵暗号方式は、適当な長さの文字列（ブロック）ごとに同じ鍵で暗号化するブロック暗号と文字列またはビットごとに鍵を変えていくストリーム暗号に分けることができる。ブロック暗号には文字の順序を置き換えて暗号化する転置式暗号や、文字を他の文字に置き換える換字式暗号等がある。この場合、転置や換字の対応表が暗号鍵となる。

【0069】ストリーム暗号には多表を用いるビジネル暗号や1回限りの使い捨ての鍵を用いるバーナム暗号等が知られている（各暗号の詳細は池野、小山著「現代暗号理論」電子情報通信学会、1986、の第2章及び第4章参照）。また、ブロック暗号のなかでもアルゴリズム

が公開されているDES(Data Encryption Standard)やFELA(Fast data Encipherment ALgorithm)といった暗号（詳細は辻井、笠原著「暗号と情報セキュリティ」昭晃堂、1990、の第2章参照）が商用暗号として広く用いられている。

【0070】ただし、DESやFELAはアルゴリズムを公開しているために暗号解読法も開発され、その解読法に対抗するために種々の変形が行われていることがある（例えば、後述の繰り返し回数を増したり(C. H. Mayer and S. M. Matyas: "CRYPTOGRAPHY-A New Dimension in Computer Data Security", Wiley-Interscience, Appendix D, pp. 679-712, 1982参照)、鍵を頻繁に変える(山本、岩村、松本、今井:

"2乗型疑似乱数生成器とブロック暗号を用いた実用的暗号方式", 信学技報, ISEC93-29, pp. 65-75, 1993. 参照)などの変形が提案されている)。

【0071】[公開鍵暗号方式] 公開鍵暗号方式は暗号鍵と復号鍵が異なり、暗号鍵を公開、復号鍵を秘密に保持する暗号方式である。以下公開鍵暗号について(a)で特徴、(b)でプロトコル、(c)で代表例、(d)で具体的な方式としてRSA暗号についてそれぞれ述べる。

【0072】(a) 公開鍵暗号の特徴

(1) 暗号鍵と復号鍵とが異なり暗号鍵を公開できるため、暗号鍵を秘密に配送する必要がなく、鍵配送が容易である。

(2) 各利用者の暗号鍵は公開されているので、利用者は各自の復号鍵のみ秘密に記憶しておけばよい。

(3) 送られてきた通信文の送信者が偽物でないこと及びその通信文が改ざんされていないことを受信者が確認するための認証機能を実現できる。

【0073】(b) 公開鍵暗号のプロトコル

通信文*M*に対して、公開の暗号鍵*Kp*を用いた暗号化操作を*E(kp, M)*とし、秘密の復号鍵*ks*を用いた復号操作を*D(ks, M)*とすると、公開鍵暗号アルゴリズムは、まず次の2つの条件を満たす。

【0074】(1) *kp*が与えられたとき、*E(kp, M)*の計算は容易である。*ks*が与えられたとき、*D(ks, M)*の計算は容易である。

(2) もし、*ks*を知らないなら、*kp*と*E*の計算手順と  $C = E(kp, M)$ を知っていても、*M*を決定することは計算量の点で困難である。次に、上記(1)、(2)に加えて、次の(3)の条件が成立することにより秘密通信が実現できる。

【0075】(3) 全ての通信文(平文)*M*に対し、*E(kp, M)*が定義でき、*D(ks, E(kp, M))*

10

20

30

40

50

=Mが成立する。つまり、 $k_p$ は公開されているため誰もが $E(k_p, M)$ を計算することができるが、 $D(k_s, E(k_p, M))$ を計算してMを得ることができるのは秘密鍵 $k_s$ を持っている本人だけである。一方、上記(1)、(2)に加えて、次の(4)の条件が成立することにより認証通信が実現できる。

【0076】(4)すべての通信文(平文)Mに対し、 $D(k_s, M)$ が定義でき、 $E(k_p, D(k_s, M)) = M$ が成立する。つまり、 $D(k_s, M)$ を計算できるのは秘密鍵 $k_s$ を持っている本人のみであり、他の人が偽の秘密鍵 $k_s'$ を用いて $D(k_s', M)$ を計算し、 $k_s$ を持っている本人になりすましたとしても、 $E(k_p, D(k_s', M)) \neq M$ なので受信者は受けとった情報が不正なものであることを確認できる。また、 $D(k_s, M)$ が改ざんされても $E(k_p, D(k_s, M)') \neq M$ となり、受信者は受けとった情報が不正なものであることを確認できる。

【0077】公開鍵暗号では、公開鍵を用いる処理Eを暗号化、秘密鍵を用いる処理Dを復号と呼んでいる。従って、秘密通信では送信者が暗号化を行い、その後受信者が復号を行うが、認証通信では送信者が復号を行い、その後受信者が暗号化を行うことになる。

【0078】以下に公開鍵暗号により送信者Aから受信者Bへ秘密通信、認証通信、署名付秘密通信を行う場合のプロトコルを示す。Aの秘密鍵を $k_{sA}$ 、公開鍵を $k_{pA}$ とし、Bの秘密鍵を $k_{sB}$ 、公開鍵を $k_{pB}$ とする。

【0079】[秘密通信] AからBへの通信文(平文)Mを秘密通信する場合次の手順で行う。Step1: AはBの公開鍵 $k_{pB}$ でMを暗号化し、暗号文CをBに送

る。  
 $C = E(k_{pB}, M)$

Step2: Bは自分の秘密鍵 $k_{sB}$ でCを復号し、もとの平文Mを得る。

$H = D(k_{sB}, C)$

受信者Bの公開鍵は不特定多数に公開されているので、Aに限らず全ての人がBに秘密通信できる。

【0080】[認証通信] AからBへの通信文(平文)Mを認証通信する場合次の手順で行う。Step1: Aは自分の秘密鍵 $k_{sA}$ で送信文Sを生成しBに送

る。  
 $S = D(k_{sA}, M)$

この送信文Sを署名文といい、署名文を得る操作を署名という。Step2: BはAの公開鍵 $k_{pA}$ でSを復元変換し、もとの平文Mを得る。

$M = E(k_{pA}, S)$

もしMが意味のある文であることを確認したならば、Mが確かにAから送られてきたことを認証する。送信者Aの公開鍵は不特定多数に公開されているので、Bに限らず全ての人がAの署名文を認証できる。このような認証をデジタル署名ともいう。

【0081】[署名付秘密通信] AからBへの通信文(平文)Mを署名付秘密通信する場合次の手順で行う。

Step1: Aは自分の秘密鍵 $k_{sA}$ でMを署名し、署名文Sを作る。

$S = D(k_{pA}, M)$

さらにAはBの公開鍵 $k_{pB}$ でSを暗号化し、暗号文CをBに送る。

$C = E(k_{pB}, S)$

Step2: Bは自分の秘密鍵 $k_{sB}$ でCを復号し、署名文Sを得る。

$S = D(k_{sB}, C)$

さらに、BはAの公開鍵 $k_{pA}$ でSを復元変換し、もとの平文Mを得る。

$M = E(k_{pA}, S)$

もし、Mが意味のある文であることを確認したならば、Mが確かにAから送られてきたことを認証する。

【0082】なお、署名付秘密通信の各Step内における関数を施す順序はそれぞれ逆転してもよい。すなわち、上記の手順では、

Step1:  $C = E(k_{pB}, D(k_{sA}, M))$

Step2:  $M = E(k_{pA}, D(k_{sB}, C))$

となっているが、下記のような手順でも署名付秘密通信が実現できる。

Step1:  $C = D(k_{sA}, E(k_{pB}, M))$

Step2:  $M = D(k_{sB}, E(k_{pA}, C))$

(c) 代表的な公開鍵暗号方式

【0083】次に代表的な公開鍵暗号方式の例を以下に挙げる。秘密通信と認証通信ができる方式として

・RSA暗号(R. L. Rivest, A. Shamir and I. Adleman: "A method of obtaining digital signatures and public key cryptosystems", Comm. of ACM, 1978)、

・R暗号(M. Rabin: "Digitalized signatures and public-key cryptosystems", MIT/LCS/TR-212, Technical Report MIT, 1979)、

・W暗号(H. C. Williams: "A modification of the RSA public-key encryption procedure", IEEE Trans. Inf. Theory, IT-26, 6, 1980)、

・MI暗号(松本、今井: "公開鍵暗号系の新しいアルゴリズム", 信学技報, IT82-84, 1982:

T. Matsumoto and H. Imai: "A class of asymmetric cryptosystems based on polynomials over finite rings",

・IEEE International Symp. on Information Theory, 1983).

・【0084】秘密通信のみができる方式として

・MH暗号(R. C. Merkle and M. E. Hellman: "Hiding information and signatures in trapdoor knapsacks", IEEE Trans. Inf. Theory, IT-24, 5, 1978).

・GS暗号(A. Shamir and R. E. Zippel: "On the security of the Merkle-Hellman cryptographic scheme", IEEE Trans. Inf. Theory, IT-26, 3, 1980).

・CR暗号(B. Chor and R. L. Rivest: "A knapsack type public key cryptosystem based on arithmetic in finite field", Proc Crypto 84).

・M暗号(R. J. McEliece: "A public-key cryptosystem based on algebraic coding theory" DSN Progress Rep. Jet Propulsion Lab 1978).

・E暗号(T. E. ElGamal: "A public key cryptosystem and a signature scheme based on discrete logarithm", Proc Crypto 84, 1984).

・T暗号(辻井重男, "行列分解を利用した公開鍵暗号の一方式", 信学技報, IT8512, 1985).

・【0085】認証通信のみができる方式として

・S暗号(A. Shamir: "A fast signature scheme", Report MIT/LCS/TM-107, MIT laboratory for computer science Cambridge, Mass, 1978).

・L暗号(K. Lieberherr: "Uniform complexity and digital signature" Lecture Notes in Computer Science 115 Automata Language and Programming, Eighth Colloquium Acre, Israel, 1981).

・GMY暗号(S. Goldwasser, S. Micali and A. Yao: "Strong signature schemes", ACM Symp. on Theory of Computing, 1983).

・GMR暗号(S. Goldwasser, S. Micali and R. L. Rivest: "A paradoxical solution to the signature problem", ACM Symp. on Foundation of Computer Science, 1984).

・OSS暗号(H. Ong, C. P. Schnorr and A. Shamir: "An efficient signature scheme based on quadratic equation", ACM Symp. on Theory of Computing, 1984).

・OS暗号(岡本、白石: "多項式演算によるデジタル署名方式", 信学論(D), J86-D, 5, 1985; T. Okamoto and A. Shiraishi: "A fast signature scheme based on quadratic inequalities" IEEE Symp. on Theory of Computing, 1984).

などをはじめ様々な方式が提案されている。

【0086】

【発明の効果】以上説明したように、本発明によれば、マルチメディアネットワーク等における前述した(1)～(3)に示した従来の問題を解決した課金方式及び課金システムが実現できる。これによって、利用者は種々の情報をレンタル的に安価に利用しながらプライバシーの保護ができ、情報提供者は利用者毎の情報利用の管理を行うことなく、提供情報の利用頻度に応じて利用料金の分配を受けることができる。また、販売店を含む料金分配者や料金立替者を導入することによって、料金の支払いまで含めて使い勝手の良い課金システムを構成することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態を示すブロック図である。

【図2】本発明の第2の実施の形態を示すブロック図である。

【図3】本発明の第3の実施の形態を示すブロック図である。

【図4】第3の実施の形態によるネットワークのブロック図である。

【図5】本発明の第4の実施の形態を示すブロック図である。

【図6】第4、第5の実施の形態によるネットワークのブロック図である。

【図7】本発明の第5の実施の形態を示すブロック図である。

【図8】本発明の第6の実施の形態を示すブロック図である。

【図9】第6の実施の形態によるネットワークのブロック図である。

【図10】従来の超流通方式を説明するためのブロック図である。

【符号の説明】

P 情報提供者

PPC 金銭情報

10 利用者端末

\* 11 判定部

14 PPC入力部

16 課金部

17 信号処理部

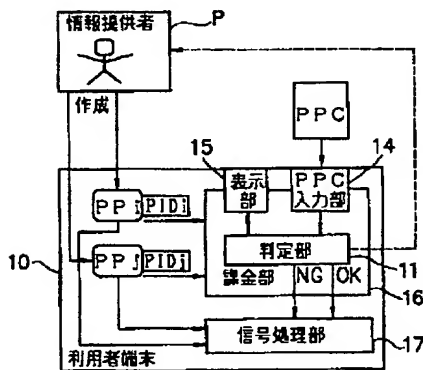
20 料金分配者

21 通信 I/F

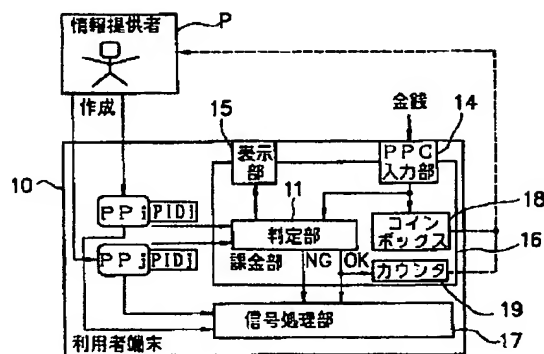
22 ネットワーク

\* 23 料金立替者

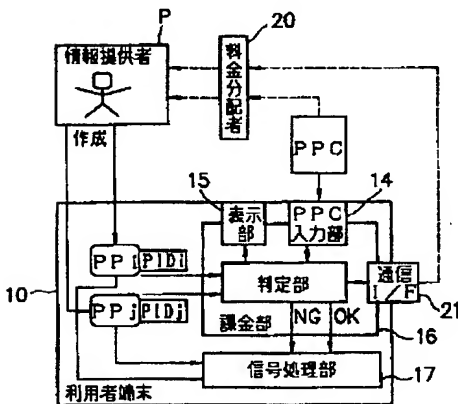
【図1】



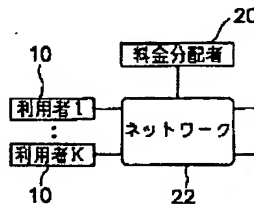
【図2】



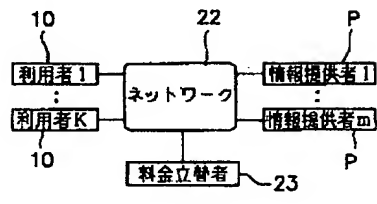
【図3】



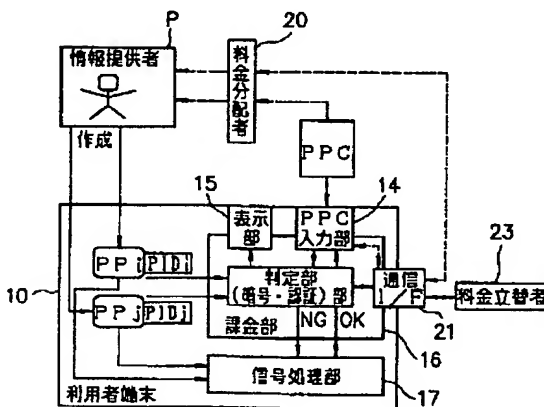
【図4】



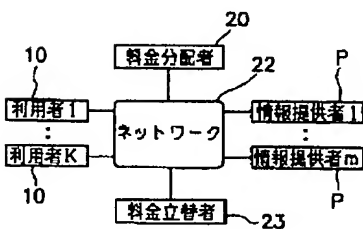
【図9】



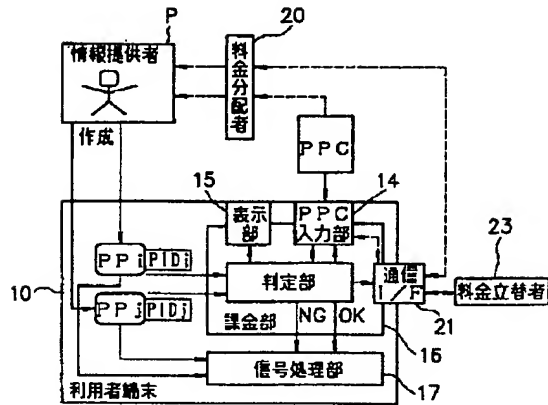
【図5】



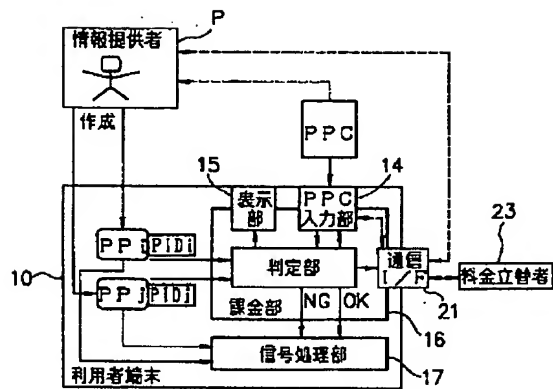
【図6】



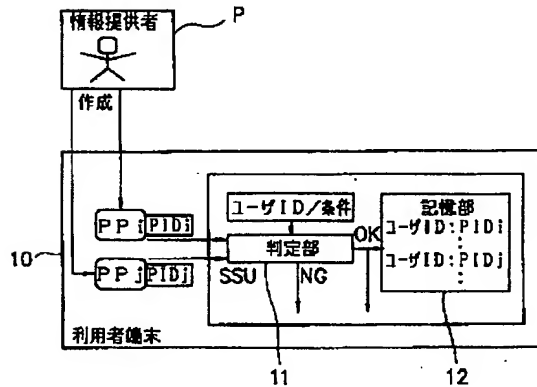
【図7】



【図8】



【図10】



フロントページの続き

(51)Int.Cl.<sup>7</sup>

G 0 6 F 17/60

G 0 6 K 17/00

G 0 7 F 17/00

識別記号

5 1 0

F I

G 0 6 F 17/60

G 0 6 K 17/00

G 0 7 F 17/00

テーマコード(参考)

5 1 0

R

B